

DEPARTMENT OF THE INTERIOR
MINERALS MANAGEMENT SERVICE MANUAL

TRANSMITTAL SHEET

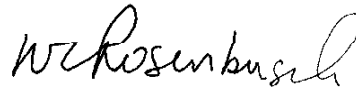
Release No. 267

January 28, 2000

Subject: Administrative Series
Part 383 Public Access to Records
Chapter 1 Privacy Act

EXPLANATION OF MATERIAL TRANSMITTED:

This release reflects an update of requirements issued in the Office of Management and Budget Circular A-130; Appendix 1--Federal Agency Responsibilities for Maintaining Records About Individuals; Appendix 3--Security of Federal Automated Information Resources; and Appendix 4--Analysis of Key Sections.



Director

FILING INSTRUCTIONS:

REMOVE:

| <u>Part</u> | <u>Chapter</u> | <u>Pages</u> | <u>Release</u> |
|-------------|----------------|--------------|----------------|
| 383 | 1 | 1-28 | 127 |

INSERT:

| <u>Part</u> | <u>Chapter</u> | <u>Pages</u> | <u>Release</u> |
|-------------|----------------|--------------|----------------|
| 383 | 1 | 1-16 | 267 |

OPR: Information Resources Management Division
Office of Administration and Budget

DEPARTMENT OF THE INTERIOR
MINERALS MANAGEMENT SERVICE MANUAL

Administrative Series

Part 383 Public Access to Records

Chapter 1 Privacy Act

383.1.1

1. Purpose. To establish responsibilities and provide guidance for implementation of the Privacy Act within the MMS.

2. Authority.

- A. Privacy Act of 1974 (5 U.S.C. 552a),
- B. Departmental Privacy Act Regulations (43 CFR 2, Subpart D), and
- C. Departmental Manual (383 DM 1-12, Public Access to Records).

3. Responsibilities.

A. All Associate Directors, the Regional Directors, and the Administrative Service Center Managers are responsible for:

- (1) reporting a system of records to the MMS Privacy Act Officer;
- (2) designating a system manager for each system of records maintained;
- (3) reporting any change in recordkeeping practices of systems of records to the MMS Privacy Act Officer; and
- (4) ensuring that individuals are allowed to exercise their rights under the Privacy Act as quickly and with as few procedural difficulties as possible.

B. The Associate Director for Administration and Budget is responsible for implementing the requirements of the Privacy Act within the MMS by:

- (1) designating an MMS Privacy Act Officer and
- (2) reporting the name, title, address, and telephone number of the MMS Privacy Act Officer to the Departmental Privacy Act Officer.

OPR: Information Resources Management Division
Office of Administration and Budget

Supersedes Release No. 127
Date: January 28, 2000 (Release No. 267)

Page 2

DEPARTMENT OF THE INTERIOR
MINERALS MANAGEMENT SERVICE MANUAL

Administrative Series

Part 383 Public Access to Records

Chapter 1 Privacy Act

383.1.3.C

C. The MMS Privacy Act Officer carries out the responsibility of the Associate Director for Administration and Budget for implementing the requirements of the Privacy Act by:

- (1) providing guidance and assistance to MMS personnel concerning the Privacy Act;
 - (2) serving as liaison with the Department on all Privacy Act matters;
 - (3) identifying all systems of records maintained;
 - (4) ensuring that system notices are current;
 - (5) ensuring the proper maintenance and safeguarding of all systems of records;
 - (6) compiling and submitting the annual Privacy Act Report to the Department;
 - (7) reviewing and concurring with the system manager's issuance of denials or partial denials of request from individuals for notification, access, or amendment;
 - (8) reviewing annually the internal policies and procedures used to implement requirements of the Privacy Act within the MMS; and
 - (9) conducting or directing periodic inspections of areas where records subject to the Privacy Act are maintained.
4. External Directive – The Departmental Manual (383DM 1-12, Public Access to Records) is hereby incorporated by reference.

SAFEGUARDING OF PRIVACY ACT RECORDS FOR AUTOMATED SYSTEMS

The Privacy Act of 1974 imposes numerous requirements upon federal agencies to prevent the misuse or compromise of data concerning individuals. Data concerning individuals should be provided a reasonable degree of protection against unauthorized disclosure, destruction, or modification, whether intentionally caused or resulting from an accident or carelessness. The following computer security risk assessment and safeguard procedures will be implemented by the system managers in accordance with the Act.^{1/}

Security Risk Assessment. Identify and prioritize those vulnerabilities which could compromise the integrity and confidentiality of data concerning individuals.

A. Degree of Risk. Estimate the degree of risk in quantitative terms. Inexact estimates of risks are still adequate for the purpose of selecting appropriate safeguards. The following procedures are to be used in estimating risks:

(1) expected frequency of accidental risks should be based on previous experience of MMS and/or other agencies with similar records systems.

(2) estimate the cost of carrying out the threat of risks that arise from deliberate acts.

(3) estimate possible individual benefits when considering risks of unauthorized access.

B. Risk Assessment Team. A risk assessment team should be established and be comprised of the following representatives:

(1) the operating unit supported by or having jurisdiction over the data under consideration (system of records); i.e., system manager;

(2) the unit responsible for managing IT operations; i.e., Information Resources Management Division; and

(3) the person assigned the responsibility for overseeing or auditing system security, the Installation IT Security Officer (IITSO).

^{1/} The ADP risk analysis conducted in accordance with MMSM 306.7, ADP Security Program, will suffice the requirements for risk assessments on systems of Privacy Act records maintained by sensitive computer installations, as presented in this appendix.

C. For purposes of this appendix, the following definitions will apply:

- (1) Encryption is the process of transforming readable plain text information, using a secret key, into unreadable cipher text.
- (2) Risks are exposures to the chance of loss.
- (3) Threats are indicators of probable loss.
- (4) Vulnerabilities are weaknesses.

D. Categories of Security Risks to be Considered. Risks must be assessed with respect to every file of information in the system concerning individuals. Each system manager in conjunction with the IITSO will have to identify the specific risks for the system and evaluate the impact of those risks in terms of the system's information files. The following categories are to be considered in selecting categories specific to a particular system:

- (1) accidents, errors, and omissions; e.g., input error, program errors, mistaken processing of data, data loss, improper data dissemination, or careless disposal;
- (2) risks from uncontrolled system access, such as open system access, theft of data, unprotected files, remote access, and open access during abnormal circumstances; and
- (3) risks from authorized users of personal data. Practices which contribute to these risks include:
 - (a) poorly defined criteria for authorized access,
 - (b) lax attitude toward employee dishonesty, and
 - (c) unaudited access to personal data.
- (4) Risks from the physical environment and from malicious destructive acts. This is not usually a primary risk for disclosure; however, such acts may destroy records required by the Privacy Act, or may damage accuracy or timeliness. Examples of these include fire, heat, water damage, flood, electric power failure, and malicious destruction by employees or outsiders.

- (5) Risks from unauthorized access. These risks include:
- (a) misidentified access (uncontrolled passwords);
 - (b) operating system flaws;
 - (c) subverting programs (programs containing hidden subprograms that disable security protections);
 - (d) spoofing (actions taken to mislead system personnel of the system software into performing an operation that appears normal but actually results in unauthorized access); and
 - (e) eavesdropping (communication lines monitored by unauthorized terminals to obtain or modify information or to gain unauthorized access to an IT system).

E. Cost/Benefit Considerations for Selecting Safeguards. Consideration should be given to the cost of each safeguard when selecting options.

- (1) initial costs include:
 - (a) purchase of new system components,
 - (b) modification of existing systems to accept the new component,
 - (c) administrative measures to support the components, and
 - (d) initial testing of their effectiveness.
- (2) Operating costs include increased day-to-day costs of running the enhanced system including such cost components as personnel, computer processing, storage, and system monitoring.
- (3) Costs of security measures for ensuring privacy should, wherever feasible, be kept separate from costs of security measures installed for other reasons.
- (4) Each protective measure should be assessed in terms of the incremental protection achieved by the additional cost.

F. Physical Security. Physical security as it pertains to the protection of data should include the following considerations:

- (1) Entry Controls.
 - (a) Limit the number of entrances to the computer facility to a minimum.

- (b) Install a screening device at every entrance; i.e., guard, badge reader, electric lock, TV camera, or a physical lock.
- (c) Monitor closely all items moving into or out of the facility.
- (d) Secure all openings through which an intruder could gain entrance or receive material.
- (e) Control the use of badges to permit entry. Visitors should be issued temporary badges differing in appearance from employee badges. In conducting an exit clearance, it is essential to retrieve all badges, keys, etc.
- (f) In case of any unusual diversions such as power outages, bomb threats, or false fire alarms, make a thorough search of the facility to prevent or uncover loss or destructive activity which might have taken place during any confusion, when loss of life or injury to an employee is not a threat.
- (g) Provide adequate protection for remote terminals, tape libraries, trash areas, etc., which are not within the confines of the computer facility.

(2) Storage Protection.

- (a) Devise fire protection plans with data storage media in mind: i.e., risks which firefighting imposes on stored data. Tape and disk library vaults will have a 25 percent protection rating and design which keeps contents safe from steam and water damage.
- (b) Arrange for separate offsite storage for computer printouts, records of disclosure, and source material.
- (c) Provide protective plastic coverage if data are vulnerable to water.
- (d) Conduct frequent unscheduled security inspections.

G. Information Management Practices. These include data collection, validation, and transformation; information processing or handling; recordkeeping; information control, display, and presentation; and standardization of information management operations. The information management guidelines below are grouped into major categories to facilitate the expansion of their role. Selection of practices from those identified below should reflect their relevance to the specific environment.

(1) Handling of Personal Data.

(a) Prepare a procedures handbook which describes the precautions to be used and obligations of computer facility personnel during the physical handling of all data about individuals. Include a reference regarding the applicability of the procedures to those government contractors who are subject to the Privacy Act.

(b) Externally label all recording media which contain data subject to the Privacy Act.

(c) Store Privacy Act data in a manner that conditions users to respect their confidentiality.

(d) If a program generates reports containing data about individuals, have the program print clear warnings of the presence of such data on the reports or manually hand-stamp all reports/output.

(e) Color code all computer input/output media, such as cd-roms, tapes, or diskettes which contain Privacy Act data.

(f) Carefully control products of intermediate processing steps to ensure that they do not contribute to unauthorized disclosure of data about individuals.

(g) Maintain an up-to-date hard copy authorization list of all individuals (computer personnel as well as system users) allowed to access control and authorization validation.

(h) Maintain an up-to-date data dictionary listing the complete inventory of Privacy Act data files within the information technology facility in order to account for all obligations and risks.

(2) Data Processing Practices.

(a) Verify the accuracy of individual data acquisition and entry methods.

(b) Conduct both regular and unscheduled inventories of all media to ensure accurate accounting for all data about individuals.

(c) Use carefully devised backup procedures for Privacy Act data. A copy of the data should be kept at a second location if their maintenance is required by law.

(d) Create a records retention timetable covering all Privacy Act data and minimally stating the data type, the retention period, and the authority responsible for making the retention decision.

(e) After a computer failure, users are to check all Privacy Act data which were being processed at the time of failure for inaccuracies resulting from the failure.

(f) If the data volumes permit economic processing, some sensitive applications may use a dedicated processing period.

(3) Programming Practices.

(a) Wherever possible, subject all programming development and modification to independent checking.

(b) Inventory current programs which process or access Privacy Act data; verify their authorized usage.

(c) Enforce programming practices which make the use of Privacy Act data in any computer program or web page clearly and fully identified.

(d) When access to the operating system exists, strictly control and require written authorization for all operating system changes that involve software security.

(4) Assignment of Responsibilities.

(a) The IITSO is responsible for examining installation practices in storage, use and processing of Privacy Act data including the use of physical security measures, information management practices, and computer system access controls. The individual should consider both internal uses and the authorized external transfer of data, reporting any risks to the relevant management authority.

(b) The regional and local IT staffs are responsible for ensuring that the facility is adequately manned with competent personnel and that the policies for the protection of Privacy Act data are enforced.

(c) All employees engaged in the handling or processing of Privacy Act data are responsible for adhering to established conduct and safeguard procedures.

(5) Procedural Auditing. Whenever appropriate, conduct an independent examination of established procedures. Audits of both specific information flow and general practices are possible. The following points should be considered when developing an audit:

(a) Auditing groups should be established within specified organizational units to provide ensurance of compliance. These groups should be independent of those directly responsible.

(b) Independent outside auditors can be contracted to provide similar ensurance at irregular intervals.

(c) Audit reports should be maintained for routine inspection and to provide additional data for tracing compromises of confidentiality.

H. Systems Security. This includes user identification procedures, access auditing to trace activity in the system, and system mechanisms to control data access, all of which can be incorporated into MMS systems.

(1) Identification. There are three categories of methods by which a person's identity may be established for the purpose of allowing access to an information system. The methods, which can be applied singly or in combination, are based on:

(a) something the person know such as passwords, combinations to locks, and series of facts from an individual's personal background:

(b) something the person has such as badges, cards with machine-readable information, and keys to locks; or

(c) something the person is such as the person's appearance, fingerprints, hand geometry, voice, or signature.

(2) System Access Controls.

(a) Passwords.

(i) should be used not only to identify users, but also to control which data and other system resources they are authorized to use;

(ii) should be easy to remember, but should not be based on information such as a person's initials or birth date; and

(iii) Should be changed at given intervals, as well as whenever compromise is known or suspected.

(b) Commercially available systems may have data access controls built in.

(c) Application programs can have their own access control mechanisms built in if the operating system does not provide them.

(3) Access Auditing. Audit trails should be designed to list all system activity, all data accesses, unusual activity, etc. Such a report can be examined for unauthorized disclosures of data.

(4) Network Systems. Suggested considerations are as follows:

(a) Establish requirements for identification, access control, and access auditing methods;

(b) Establish controls on network access; and

(c) Verify special requests involving sensitive data to the computer operating system, even though initial system access has been granted to the operator.

(5) Data Encryption.

(a) Control devices must be constructed to format the data for the encryption device and to transmit and receive the encrypted data.

(b) Locate encryption devices so as to protect Privacy Act data at places where data are vulnerable to network security threats.

(c) Data encryption keys must be created and distributed to authorized network personnel. These keys must be protected at all times and changed frequently.

GENERAL INFORMATION AND GUIDELINES
FOR EMPLOYEES PROCESSING REQUESTS FOR
RECORDS IN SYSTEMS SUBJECT TO THE PRIVACY ACT

Introduction

To claim the rights afforded by the Privacy Act, an individual must follow the formal procedures established by the Department's regulations (43 CFR 2, Subpart D). Bureaus, however, may honor requests for notification, access, or amendment that do not meet the requirements of the regulations. THE SYSTEM MANAGER MAY ISSUE INSTRUCTIONS PROVIDING FOR RESPONDING TO INFORMAL REQUESTS. THIS SET OF GUIDELINES ASSUMES A FORMAL REQUEST BY THE INDIVIDUAL UNDER THE PROVISIONS OF THE PRIVACY ACT.

In carrying out the instruction in this guideline, keep in mind that individuals making requests under the Privacy Act are exercising rights granted by the Act. Responses, therefore, should be appropriate to these rights. Courtesy is a natural requirement. Equally important is the ease with which individuals are able to exercise these rights. It is Departmental policy to facilitate the exercise of Privacy Act rights. Inquiries from individuals shall be responded to as quickly and with as few procedural difficulties as possible.^{1/}

STEP 1: Response to Inquiries about the Existence of Personal Records

The Privacy Act recognizes that individuals must be aware that certain systems of records exist before they can determine whether the system contains data about them. Therefore, the Act requires publication of a notice describing each system of records containing information accessible by an individual's name, identifying number, symbol, or other identifier.

This system notice both describes the system and explains how individuals can determine whether the system contains information pertaining to them. Generally, individuals need only to provide their names for such a check. In some cases, however, other information is needed for locating records (e.g., social security number). In these cases, the system notice will specify the additional information necessary for access.

^{1/} Certain personnel records used for personnel management programs or processes are administered under the authority of the Office of Personnel Management and are maintained under security requirements prescribed in OPM regulations (5 CFR 293).

Departmental regulations (43 CFR 2.60) require that requests invoking the Privacy Act be in writing.^{2/} These requests should be marked "Privacy Act inquiry" to ensure expeditious handling, should identify the system of records to which the inquiry pertains, and should comply with other requirements set forth in the system notice. Requests may be mailed or delivered personally to the location given in the system notice.

Upon receiving the request, determine if the request meets the above-noted requirements. If it does, then carry out the following steps:

- A. Determine whether records on that individual are maintained in the files.
- B. Determine if the records contain information gathered in reasonable anticipation of a civil action or if they are exempt from notification under a rule adopted by the Secretary. If either of these conditions apply, notify the system manager through the channels provided in your system. The system manager is responsible for notifying the individual in these cases. **UNDER NO CIRCUMSTANCES SHOULD THE INQUIRING INDIVIDUAL BE ADVISED THAT THE RECORD EXISTS OR THAT THERE IS A RESTRICTION ON NOTIFICATION.**
- C. If records are found not subject to the exemptions noted in paragraph B above, determine the types of records and prepare a response to the individual that identifies the records being kept so the individual may choose which ones they wish to inspect. (This does not mean that the individual has a right to inspect the records because they still may be exempt from inspection. However, the individual has a right to know that they exist.)
- D. If no records are found, advise the individual.

STEP 2: Request to Inspect Records

This step may or may not have been preceded by the procedures described above. Often an individual knows that records exist on them in the system and may directly request access to them. Like an inquiry concerning the existence of records,

^{2/} Requests for notification, access, or amendment that do not conform to the requirements in 43 CFR 2.60, such as oral requests, may be honored as a matter of administrative discretion. It is not necessary to require individuals to invoke the Privacy Act. (see 383 DM 6.3.)

requests for access must be in writing. They should also be marked "Privacy Act Request for Access" and should contain the information required by the regulations and the system notice.

Upon receiving a Privacy Act request for access, carry out the following steps:

A. Determine the individual's identity. Usually the signature on the letter or an identification card will suffice. If additional identification is required, the system manager will so inform you.

B. Determine whether the requested records are open for inspection by the individual. The Privacy Act requires that records be available for inspection unless compiled in reasonable anticipation of a civil action or proceeding or exempted by a rule adopted by the Secretary. The system manager is responsible for giving guidance on how to handle records that are exempted from the access provisions of the Act. Ascertain whether an exemption has been claimed for the requested records. Ask the system manager or read the system notice which has been published for the records system if in doubt.

C. If the records are open for inspection by the individual, retrieve the records and make them available to the individual in a space suitable for such inspection.^{3/}

(1) If the individual is accompanied by a third party who also is to see the records, obtain a written, signed statement from the individual whose records are being examined stating that the other party may be present during the inspection.

(2) If the request to inspect the records specified that the inspection was to be through copies of the record to be sent to the individual, the request should also state the amount of money the individual is willing to pay for the copies.

^{3/} The Privacy Act gives the individual the right to see their records unless they are exempted. An access request must be acted on promptly. The MMS cannot plead cost or workload burden as a reason for not making the records available or for taking a long time to respond. The MMS cannot charge the individual for any costs related to making the information and records available, unless copies have been requested. In those cases, only the copying cost may be charged.

(a) The system manager should provide a schedule of charges for copies of the records. If this schedule is not available, obtain it from the system manager. Determine the number of copies required and the amount to be charged. If the charge equals or is less than the amount indicated in the letter, make the requested copies of the record, and send them to the individual along with a bill for collection (DI-1040).

(b) If the cost exceeds the stipulated amount, advise the individual of the full anticipated cost and costs for portions of the record (if applicable). The requester must agree in writing to pay fees as high as are anticipated before processing of the request is completed.

(c) The system manager may specify that medical records in the system are not to be shown to the individual. In such cases, copies of the medical records may be sent to a physician of the individual's choice upon the receipt of a letter from the physician requesting the file on the part of the individual. That physician will then decide whether to reveal the contents of the medical record to the individual. There is no charge for such copies, even if the physician retains them.

STEP 3: Requests for Amendment

The Privacy Act provides certain safeguards for an individual against an invasion of personal privacy. It requires, among other things, that agencies collect, maintain, use, or disseminate any record of identifiable information about an individual in a manner that ensures that such action is for a necessary and lawful purpose, that the information is current and accurate for its intended use, and that adequate safeguards are provided to prevent misuse of such information. If on inspection of their records, the individual thinks that the records contain information inconsistent with the above requirements, they may request that information be corrected or removed from the files.

The system manager is responsible for determining whether the information in the files is relevant, necessary, and accurate. Since these three conditions are not always clear-cut, there is a strong possibility that individuals will disagree with what is in their records and want it removed or changed under one of the above three criteria. The Privacy Act requires that requests for amendment be responded to or acknowledged in 10 days. Thus, prompt action is needed.

A petition for amendment must be submitted in writing to the system manager. It is likely that an employee's involvement in amending records will be through inquiry to and instruction from the system manager.

In some cases, individuals personally inspecting their records may see routine information such as an address or a telephone number that is incorrect. IF YOUR SYSTEM MANAGER HAS PROVIDED GUIDELINES AUTHORIZING SUCH CHANGES IN THE RECORDS, YOU MAY MAKE THEM IN ACCORDANCE WITH THE GUIDELINES.